Making Cyber Security a Cultural Norm

AMC/A6OS
DSN 779-6298

Raising Digital Citizens

- **Remain positively engaged:** Pay attention to and know the online environments your children use.
- **Teach critical thinking:** Help your children identify safe, credible Web sites and other digital content, and be cautious about clicking on, downloading, posting, and uploading content.
- **Help them be good digital citizens:** Remind your children to be good "digital friends" by respecting personal information of friends and family and not sharing anything about others that is potentially embarrassing or hurtful.
- **Know the rules:** Not all online services are for kids.
- **If you know of a child in immediate risk or danger, call law enforcement right away.** Report instances of online child exploitation to the National Center For Missing and Exploited Children's Cyber Tipline. Reports may be made 24-hours a d
  v 00-
  h

Home Cyber Security Culture

- **National Cyber Security Alliance Mission:** To educate and empower our global digital society to use the Internet safely and securely. Propagates information and resources through StaySafeOnline.org.
- **ConnectSafely.org** has basic guidelines for teens and parents about cyberbullying, sexting, social networking, and more.
- **GetGameSmart.com** provides information and resources to help families make smart choices about what they play, browse, and watch.
- **OnGuardOnline.gov** is the FTC's main consumer-facing page to educate everyone on staying safe and secure online.
- **WebWiseKids.org** is a unique organization that offers fun, challenging and interactive simulations based on real-life criminal cases.
- **Other educational resource include:** GetNetWise.org, iKeepSafe.org, and Wired Safety.org

UNCLASSIFIED

Air Force Cyber Security Culture

- **ADLS (Advanced Distributed Learning Service):** All Air Force personnel must annually review and complete DoD IAA CyberAwareness Challenge V3.0 (ZZ133098) in order to access the AF internet.
- **DC3I (Department of Defense Cybersecurity Culture and Compliance Initiative) Memorandum, Released 30 Sep 2015:** Outlines how DoD cyber security culture will be transformed by improving human performance and accountability in mutual support of the DoD Cyber Strategy. Publication can be found at: http://www.defense.gov/News/Publications
- **US-Cert (United States Computer Emergency Readiness Team) National Cyber Awareness System:** NCAS offers a variety of information for users with varied technical expertise. Website: https://www.us-cert.gov/ncas
- **24th Air Force "The Cyber Space":** Intended to be a "one-stop-shop" of useful educational links, stories and materials for both Air Force members and the public. Website: http://www.24af.af.mil/About-Us/The-Cyber-Space

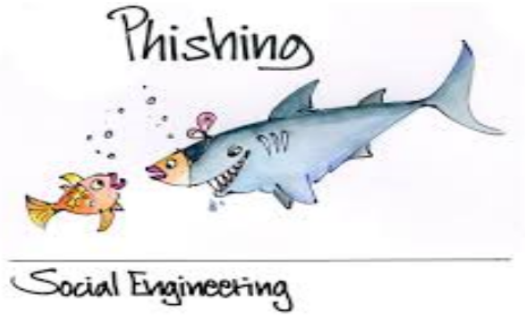
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

UNCLASSIFIED

Unrivaled Global Reach for America … ALWAYS!

Socializing Cyber Culture

- People often want to help each other and that willingness to serve can sometimes become the weak link in an enterprise's security chain.
- Social engineering attacks occur when an attacker uses human interaction and behavioral techniques to collect enough information to infiltrate an enti



- A form of Social Engineering called Phishing is today's top online threat.
- Most phishing scams demonstrate the following characteristics:
  - Seek to obtain personal information, such as names, addresses and social security numbers.
  - Use embedded links that redirect users to suspicious websites in URLs that appear legitimate.
  - Incorporates threats, fear and a sense of urgency in an attempt to manipulate the user into acting promptly.

Cyber Security Culture Breach 2015

OPM (Office of Personnel Management)

- A malware package—likely delivered via e-mail "phishing" attack against OPM or a Department of the Interior employees—managed to install itself within the OPM's IT systems and establish a back-door for further attacks. The attackers then escalated their privileges on OPM's systems to the point where they had access to a wide swath of the agency's systems.
- In April 2015, OPM discovered that the personnel data of 4.2 million current and former Federal government employees had been stolen. This means information such as full name, birth date, home address and Social Security Numbers were affected.
- While investigating this incident, in early June 2015, OPM discovered that additional information had been compromised: including background investigation records of current, former, and prospective Federal employees and contractors. OPM and the interagency incident response team have concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, len from the background investigation databases. For more tion: yber ıts/

OPM.Gov

Unrivaled Global Reach for America … ALWAYS!

Cyber Security Culture Breach 2016 Update

U.S. House Oversight and Government Reform Committee

- OPM spends $133M to provide credit monitoring services for three years to nearly 22 million people who had their Social Security numbers and other sensitive data stolen by cybercriminals
- 241-page report released (7 Sep 2016) by the U.S House Oversight and Government Reform Committee key findings:
  - The OPM data breach was preventable.
  - OPM leadership failed to heed repeated recommendations from its Inspector General, failed to sufficiently respond to growing threats of sophisticated cyber attacks, and failed to prioritize resources for cybersecurity.
  - Data breaches in 2014 were likely connected and possibly coordinated to the 201[illegible] data breach

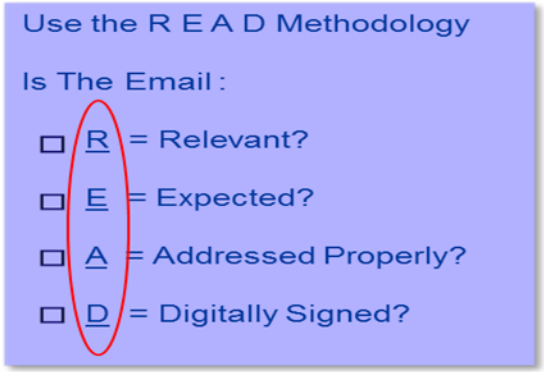
Phishing Warning Signs

- **Urgency:** Urges you to act quickly because your account may be suspended or closed.
- **Generic Greeting:** Doesn't address you by name, but uses a generic greeting like "Dear valued customer.“
- **Validate or Update Information:** Asks for account numbers, passwords or other personal information.
- **Includes Errors:** Contains misspellings or grammatical errors.
- **Unusual Content:** Is from someone you know, but includes a strange subject line or unusual attachments.
- **Unknown Link:** Contains links to unknown or suspicious websites.
- **Plausible Sender:** Claim to be from your military service, government organization, Internet service provider or bank.
- **Fake Website:** Direct you to a Website that looks real.

Protecting AF Cyber Culture

If You Receive A Suspicious Email At Work

- Do not click on ANYTHING or open any attachments.
- Open a blank email and attach the suspicious email to it.
- Send suspicious email to: 33NWS.MAN@us.af.mil
- Right-click the suspicious message in the Inbox and select Junk > Block Sender.



For AMC, we utilize the R.E.A.D. methodology:
Is your email *relevant*, *expected*, *addressed* correctly, and *digitally signed*? Know the indicators

If You Receive A Suspicious Email At Home

- Delete the if you do not know the sender.
- Report e-mails requesting personal information by contacting the possibly spoofed organization using a telephone number you know to be legitimate.
- Look for digital signatures.
- Never give out organizational, personal, or financial information to anyone by e-mail.

References

This brief and additional Information can be found here:

https://eim.amc.af.mil/sites/Cyber/default.aspx

Air Force Instruction 33-200 (31AUG15)
www.e-publishing.af.mil

POC: AMC/A6OS
DSN 779-6298